[2345/45]

Method and Device for Loading Input Data into an Algorithm When Performing an Authentication

Field of the Invention

The invention relates ~~to a method as described in detail in the preamble to Claim 1, and to a device of the kind defined in the preamble to Claim 9. Various known methods of this kind~~ are used for electronic cash cards in a plurality of variants, ~~and the devices are based, inter alia, on~~ chip circuits as described by ~~EP~~ 0 616 429 A1.

~~Methods of the kind referred to here are known~~, for example, ~~from~~ ETSI D/EN/TE 090114, Terminal Equipment (TE) Requirements for IC Cards and Terminals for Telecommunication Use, Part 4 - Payment Methods, version 4, of February 7, 1992, and from the European Patent Application 0 605 070.

In addition to phone cards, which have a defined initial credit balance as a payment means for card-operated phones, "electronic cash cards", which work according to the same principle, are gaining in significance as a means for paying limited amounts. In "pay with chip card" applications, a card reader module having a security module SM for verifying the card and the balance amount are integrated in the automatic machine.

~~EP~~ 0 605 070 A2 also describes a method for transferring credit and debit amounts to and from chip cards, memory locations of a chip card having overwrite capability being divided into at least two memory ~~locations~~ areas, one of these having a "debit function", thus acting as an "electronic purse" similarly to a phone card, and the other having a "credit function" along the lines of a credit card. To replenish the "electronic purse", provision is made for cash amounts to be transferred between the areas under the secured conditions that are typical for credit cards.

To both avoid the danger of unauthorized access to the automatic teller machines and their permanently installed security modules, as well as eliminate the need for

dedicated lines which are specially protected and, thus, expensive for the operator, ~~(P95114) proposed a method whereby~~, prior to any cash transaction, the operator of the automatic cash machine inserts a security module having chip card functions into the automatic cash ~~machine and, during~~ machine. During each cash transaction that involves a cardholder inserting his or her electronic cash card into an automatic cash machine, data areas of the chip card are first read out to permit a plausibility check and to verify the remaining credit ~~balance; after that~~ balance. Subsequently, an authentication is performed using the security module and a single or multiple acceptance decision is ~~made; and finally~~ made. Finally, the cash amount due or input is either debited to the cardholder's chip card with the aid of a security function, or added to a summing counter for cash amounts in the security ~~module; following~~ module. Following the cash transactions, the counter content of the security module having chip card functions is transferred to a clearinghouse.

Summary of the Invention

~~The~~ An object of the present invention is to further enhance the security of automatic cash machines for the electronic cash ~~purses~~ cards to prevent unauthorized manipulation and malfunctions.

~~This object is achieved in accordance with the characterizing part of Claim 1.~~

~~Advantageous variants or further developments of this method are described in the characterizing parts of dependent Claims 2 through 8.~~

~~The characterizing part of Claim 9 describes a device which is suitable for the application of the method.~~

~~The characterizing parts of dependent Claims 10 through 14 contain advantageous variants or further developments of these devices for various applications.~~

~~The invention, including its effects, advantages and fields of application, is described in detail by the following examples.~~

Authentication algorithms are typically used to enable reliable identification. Often entering into the authentication methods, besides the identity of a chip card, of a person, and possibly of a security module SM, are other data, ~~as well~~ which have to be verified. An authentication method can be applied, for example, to non-secret card data D, together with a secret key K, and a random number Z. For the sake of security when working with ~~the~~ electronic cash cards, separate security functions are used for debiting and crediting, and each of these security functions is retrieved using a cryptographic checksum.

The method of the present invention enables the debit and credit transactions to be carried out using a cryptographic token, where it is required ~~the condition being~~ that the authentication and cryptographic checksum process are performed on the counter content using a challenge/response method. A single challenge/response method can then be applied, whereby only one random number is provided by the security module SM and only one response is calculated by the chip card, to verify both the identity (authentication) as well as the internal counter content with respect to the security module SM.

This ~~can~~ may be achieved ~~in that~~ with the variable input data, such as the counter content and the random number, ~~are~~ being initially processed internally using "keyed hash ~~functions~~ functions," that is, MAC functions. In the process, the card-specific secret key of the chip card is used as the key. The two tokens extracted from counter content and the random number ~~can~~ may then be linked together, for example, (in a perhaps cryptographically unsecured way) by XOR or by using a linear-feedback shift register, and then may be output, with their integrity being protected, using a cryptographic function that is ~~strong enough~~ sufficiently powerful.

This method is of practical use ~~insofar as~~ in that the keyed hash functions, which are only used internally, do not have to meet any particularly high requirements with regard to their security, and relatively simple functions can be used since the results of these functions do not leave the chip card. Nevertheless, data manipulation is effectively prevented with this method.

An exemplary embodiment of the present invention assumes that a linear-feedback shift register (LFSR) having an additional nonlinear function and downstream counters is used. Exemplary steps and features include:

0. Additional feedback circuits are switched into the linear-feedback shift register LFSR following the downstream counters.

1. Input data, composed of the non-secret card data D and the secret key K, are read into the linear-feedback shift register LFSR, while both the feedback of the linear-feedback shift register LFSR, as well as the additional feedback(s) are active.

2. A certain number of clock pulses is processed without additional input data being read in.

3. Input data made up of the random number R are read in while both the feedback of the LFSR and the additional feedback(s) are active.

4. The additional feedback circuits are switched off, and the counters are reset, if necessary.

5. A certain number of clock pulses is processed, and, during these pulses, output bits are generated according to the current counter settings.